Foundation of Cryptography, Spring 2014 — Iftach Haitner

Problem set 3

April 10, 2014 — Due: April 29.

- Please submit the handout in class, or email me, in case you write in LaTeX
- Write clearly and shortly using sub claims if needed. The emphasize in most questions is on the proofs (no much point is writing a “solution" w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- In it ok to work in (small) groups, but please write the id list of your partners in the solution file, and each student should write his solution by *himself* (joint effort is only allowed in the “thinking phase")
- The notation we use appear in the introduction part of the first lecture (*Notation* section).

1. Prove that the proof system we presented in Lecture 6 for $\mathcal{GI}$ (Graph Isomorphism) is $\mathcal{SZK}$ against *aborting* verifiers (in class we have seen a proof for non-aborting verifiers).

2. Prove that any $\mathcal{CZK}$ protocol is also WI (Witness Indistinguishability). See definition in Slide 3 of Lecture 7.

3. Prove that WI is preserved under parallel repetition.

   Given an interactive proof (P, V) and $k \in \mathbb{N}$, the protocol $(\mathsf{P}^k, \mathsf{V}^k)$ consists of k independent executions of (P, V), where the verifier accepts if each of the k verifiers does (a cheating prover/verifier might correlate its behavior in the different executions).

   Given a WI protocol (P, V) for a language $\mathcal{L}$ and $k \in \mathbb{N}$, prove that $(\mathsf{P}^k, \mathsf{V}^k)$ is WI for $\mathcal{L}$.